IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A network adapter system, comprising:

(a) a processor positioned on a network adapter coupled between an end-point computer and a network, the network adapter capable of being installed on the end-point computer;

(b) wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses;

(c) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(d) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter.

2. (Original) The network adapter system as recited in claim 1, wherein the processor is capable of being user-configured.

3. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured locally.

4. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured remotely via a network connection with the network adapter.

5. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured only after the verification of a password.

6. (Original) The network adapter system as recited in claim 2, wherein the manner in which the scanning is performed is capable of being user-configured.

7. (Original) The network adapter system as recited in claim 2, wherein the settings of the network adapter are capable of being user-configured.

8. (Original) The network adapter system as recited in claim 1, wherein the processor is capable of determining whether received packets are of interest.

9. (Original) The network adapter system as recited in claim 8, wherein the received packets are of interest based on an associated protocol.

10. (Currently Amended) The network adapter system as recited in claim 8, wherein the processor is capable of passing received packets that are not of interest to the end-point computer.

11. (Original) The network adapter system as recited in claim 10, wherein the processor is capable of scanning received packets that are of interest.

12. (Original) The network adapter system as recited in claim 11, wherein the processor is capable of denying received packets that fail the scan.

13. (Original) The network adapter system as recited in claim 1, wherein the scan is performed based on user settings.

14. (Currently Amended) A method for scanning network traffic on a network adapter, comprising:

(a) receiving packets at a network adapter including a processor positioned thereon, the network adapter capable of being installed on an end-point computer;

(b) virus scanning and content scanning of the packets utilizing the processor, the content scanning including scanning for unwanted content other than viruses; and

(c) conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(e) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter.

15. (Original) The method as recited in claim 14, wherein the processor is capable of being user-configured.

16. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured locally.

17. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured remotely via a network connection with the network adapter.

18. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured only after the verification of a password.

19. (Original) The method as recited in claim 15, wherein the manner in which the scanning is performed is capable of being user-configured.

20. (Original) The method as recited in claim 15, wherein the settings of the network adapter are capable of being user-configured.

21. (Original) The method as recited in claim 14, wherein the processor is capable of determining whether received packets are of interest.

22. (Original) The method as recited in claim 21, wherein the received packets are of interest based on an associated protocol.

23. (Currently Amended) The method as recited in claim 22, wherein the processor is capable of passing received packets that are not of interest to the end-point computer.

24. (Original) The method as recited in claim 23, wherein the processor is capable of scanning received packets that are of interest.

25. (Original) The method as recited in claim 24, wherein the processor is capable of denying received packets that fail the scan.

26. (Original) The method as recited in claim 14, wherein the scan is performed based on user settings.

27. (Currently Amended) A system for scanning network traffic on a network adapter, comprising:

(a) network adapter means for receiving packets, the network adapter means capable of being installed on an end-point computer;

(b) processor means positioned on the network adapter means for virus scanning and content scanning of the packets, the content scanning including scanning for unwanted content other than viruses; and

(c) means for conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(e) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter means.

28. (Currently Amended) A system for scanning network traffic on a network adapter, comprising:

(a) network adapter means for receiving packets, the network adapter means being installed on an end-point computer;

(b) logic positioned on the network adapter means for virus scanning and content scanning of the packets, the content scanning including scanning for unwanted content other than viruses; and

(c) logic for conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(e) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter means.

29. (Currently Amended) A network adapter system, comprising:

(a) a processor positioned on a network adapter coupled between an end-point computer and a network, the processor including a packet assembly module, random access memory (RAM), and a scanner module, the network adapter being installed on the end-point computer;

(b) a user interface driver for identifying network traffic of interest transmitted between the end-point computer and the network;

(c) wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(e) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter.

30. (Previously Presented) The network adapter system as recited in claim 1, wherein the content scanning enforces operational policies of an organization.

31. (Previously Presented) The network adapter system as recited in claim 30, wherein the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation.

32. (Cancelled)

33. (Previously Presented) The network adapter system as recited in claim 1, wherein the memory is user protected by configuring a network adapter BIOS with a password that only a user can change.

34. (Previously Presented) The network adapter system as recited in claim 11, wherein the received packets that are of interest include executable files.

35. (New) The network adapter system as recited in claim 1, wherein the network adapter includes a Peripheral Component Interconnect (PCI) card.

36. (New) The network adapter system as recited in claim 1, wherein the network adapter includes an Industry Standard Architecture (ISA) card.

37. (New) The network adapter system as recited in claim 1, wherein the network adapter includes an Integrated Services Digital Network (ISDN) adapter.

38. (New) The network adapter system as recited in claim 1, wherein the network adapter includes a cable modem adapter.

39. (New) The network adapter system as recited in claim 1, wherein the network adapter includes a broadband adapter.

40. (New) The network adapter system as recited in claim 1, wherein the unwanted content is selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation.

41. (New) The network adapter system as recited in claim 1, wherein the unwanted content includes harassing content, pornographic content, junk e-mails, and misinformation.